

Jun 23, 2023

s/ Erin Hayes

Deputy Clerk, U.S. District Court
Eastern District of Wisconsin

UNITED STATES DISTRICT COURT

for the

Eastern District of Wisconsin

In the Matter of the Search of)

(Briefly describe the property to be searched
or identify the person by name and address))information associated with six (6) Facebook)
accounts, described further in Attachment A, that is)
stored at premises controlled by Meta Platforms, Inc.)

Case No. 23-m-405 (SCD)

WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

To: Any authorized law enforcement officer

An application by a federal law enforcement officer or an attorney for the government requests the search and seizure of the following person or property located in the _____ District of _____
(identify the person or describe the property to be searched and give its location):

See Attachment A

I find that the affidavit(s), or any recorded testimony, establish probable cause to search and seize the person or property described above, and that such search will reveal (identify the person or describe the property to be seized):

See Attachment B

YOU ARE COMMANDED to execute this warrant on or before 7-7-23 (not to exceed 14 days)

☐ in the daytime 6:00 a.m. to 10:00 p.m. ☒ at any time in the day or night because good cause has been established.

Unless delayed notice is authorized below, you must give a copy of the warrant and a receipt for the property taken to the person from whom, or from whose premises, the property was taken, or leave the copy and receipt at the place where the property was taken.

The officer executing this warrant, or an officer present during the execution of the warrant, must prepare an inventory as required by law and promptly return this warrant and inventory to _____
Honorable Steven C. Dries
(United States Magistrate Judge)☐ Pursuant to 18 U.S.C. § 3103a(b), I find that immediate notification may have an adverse result listed in 18 U.S.C. § 2705 (except for delay of trial), and authorize the officer executing this warrant to delay notice to the person who, or whose property, will be searched or seized (check the appropriate box)☐ for _____ days (not to exceed 30) ☐ until, the facts justifying, the later specific date of _____

Date and time issued: 6-23-23. 10:40 am

Stephen C. Dries
Judge's signature

City and state: Milwaukee, Wisconsin

U.S. Magistrate Judge Steven C. Dries
Printed name and title

Return		
Case No.:	Date and time warrant executed:	Copy of warrant and inventory left with:
Inventory made in the presence of :		
Inventory of the property taken and name(s) of any person(s) seized:		
Certification		
<p>I declare under penalty of perjury that this inventory is correct and was returned along with the original warrant to the designated judge.</p> <div style="display: flex; justify-content: space-between; align-items: flex-end;"> <div style="width: 30%;"> <p>Date: _____</p> </div> <div style="width: 65%;"> <p style="text-align: center;">_____</p> <p style="text-align: center;"><i>Executing officer's signature</i></p> <p style="text-align: center;">_____</p> <p style="text-align: center;"><i>Printed name and title</i></p> </div> </div>		

ATTACHMENT A

Property to Be Searched

This warrant applies to information associated with Facebook accounts:

- I. **Facebook Account: Latonya Baker, URL: www.facebook.com/fergusonbaker
(Target Account 1)**
- II. **Facebook Account: Melissa Bonds, URL:
www.facebook.com/melissa.bonds.92 (Target Account 2)**
- III. **Facebook Account: Grisel Delgado, URL: www.facebook.com/mills.finest1
(Target Account 3)**
- IV. **Facebook Account: Inez Johnson, URL: www.facebook.com/inez.a.johnson
(Target Account 4)**
- V. **Facebook Account: Alicia Washington, URL:
www.facebook.com/alicia.sanders.967 (Target Account 5)**
- VI. **Facebook Account: Eili J. Bliss, URL: www.facebook.com/eilij.cole (Target
Account 6)**

which are stored at premises owned, maintained, controlled, or operated by Meta Platforms, Inc., a company headquartered in Menlo Park, California.

ATTACHMENT B

Particular Things to be Seized

I. Information to be disclosed by Meta Platforms, Inc. (“Meta”)

To the extent that the information described in Attachment A is within the possession, custody, or control of Meta, regardless of whether such information is located within or outside of the United States, including any messages, records, files, logs, or information that have been deleted but are still available to Meta, or have been preserved pursuant to a request made under 18 U.S.C. § 2703(f), Meta is required to disclose the following information to the government for each user ID listed in Attachment A **for the time period of April 23, 2020, through the date of this warrant for Target Account 1, December 18, 2021, through the date of this warrant for Target Account 2, April 6, 2021, through the date of this warrant for Target Account 3, January 26, 2022, through the date of this warrant for Target Account 4, January 22, 2020 through the date of this warrant for Target Account 5, and August 21, 2020, through the date of this warrant for Target Account 6.**

- (a) All contact and personal identifying information, including full name, user identification number, birth date, gender, contact e-mail addresses, physical address (including city, state, and zip code), telephone numbers, screen names, websites, and other personal identifiers.
- (b) All activity logs for the account and all other documents showing the user’s posts and other Facebook activities from April 23, 2020, through the date of this warrant for Target Account 1, December 18, 2021, through the date of this warrant for Target Account 2, April 6, 2021, through the date of this warrant for Target Account 3, January 26, 2022, through the date of this warrant for Target Account 4, January

22, 2020 through the date of this warrant for Target Account 5, and August 21, 2020, through the date of this warrant for Target Account 6.

- (c) All photos and videos uploaded by that user ID and all photos and videos uploaded by any user that have that user tagged in them from April 23, 2020, to present for Target Account 1, December 18, 2021, to present for Target Account 2, April 6, 2021, to present for Target Account 3, January 26, 2022, to present for Target Account 4, January 22, 2020 to present for Target Account 5, and August 21, 2020, to present for Target Account 6, including Exchangeable Image File (“EXIF”) data and any other metadata associated with those photos and videos;
- (d) All profile information; News Feed information; status updates; videos, photographs, articles, and other items; Notes; Wall postings; friend lists, including the friends’ Facebook user identification numbers; groups and networks of which the user is a member, including the groups’ Facebook group identification numbers; future and past event postings; rejected “Friend” requests; comments; gifts; pokes; tags; and information about the user’s access and use of Facebook applications;
- (e) All records or other information regarding the devices and internet browsers associated with, or used in connection with, that user ID, including the hardware model, operating system version, unique device identifiers, mobile network information, advertising ID, and user agent string;
- (f) All other records and contents of communications and messages made or received by the user from April 23, 2020, to present for Target Account 1, December 18, 2021, to present for Target Account 2, April 6, 2021, to present for Target Account 3, January 26, 2022, to present for Target Account 4, January 22, 2020 to present

for Target Account 5, and August 21, 2020, to present for Target Account 6, including all Messenger activity, private messages, chat history, video and voice calling history, and pending “Friend” requests;

- (g) All “check ins” and other location information;
- (h) All IP logs, including all records of the IP addresses that logged into the account;
- (i) All records of the account’s usage of the “Like” feature, including all Facebook posts and all non-Facebook webpages and content that the user has “liked”;
- (j) All information about the Facebook pages that the account is or was a “fan” of;
- (k) All past and present lists of friends created by the account;
- (l) All records of Facebook searches performed by the accounts from April 23, 2020, to present for Target Account 1, December 18, 2021, to present for Target Account 2, April 6, 2021, to present for Target Account 3, January 26, 2022, to present for Target Account 4, January 22, 2020, to present for Target Account 5, and August 21, 2020, to present for Target Account 6;
- (m) All information about the user’s access and use of Facebook Marketplace;
- (n) The types of service utilized by the user;
- (o) The length of service (including start date) and the means and source of any payments associated with the service (including any credit card or bank account number);
- (p) All privacy settings and other account settings, including privacy settings for individual Facebook posts and activities, and all records showing which Facebook users have been blocked by the account;

- (q) Records of any Facebook accounts that are linked to the account by machine cookies (meaning all Facebook user IDs that logged into Facebook by the same machine as the account); and
- (r) All records pertaining to communications between Meta and any person regarding the user or the user's Facebook account, including contacts with support services and records of actions taken.

Meta is hereby ordered to disclose the above information to the government within 14 days of issuance of this warrant.

II. Information to be seized by the government

All information described above in Section I that constitutes fruits, evidence and instrumentalities of violations of 18 U.S.C. § 1956(b) (Laundering of Monetary Instruments), 18 U.S.C. § 1957 (Engaging in monetary transactions in property derived from specified unlawful activity), 18 U.S.C. § 1347 (Healthcare Fraud), 18 U.S.C. § 1035 (False Statements Related to Healthcare), 42 U.S.C. Section 1320a-7b (Illegal Kickbacks) involving LATONYA BAKER, MELISSA BONDS, INEZ JOHNSON, GRISEL DELGADO, ALICIA WASHINGTON, and SHANTERA COLE since, April 23, 2020, for Target Account 1, December 18, 2021, for Target Account 2, April 6, 2021, for Target Account 3, January 26, 2022, for Target Account 4, January 22, 2020 for Target Account 5, and August 21, 2020, for Target Account 6, including, for each user ID identified on Attachment A, information pertaining to the following matters:

- (a) Evidence demonstrating a scheme to defraud Wisconsin Medicaid; evidence demonstrating the provision of kickbacks in exchange for medical services and/or billing; evidence of communications regarding how to conduct billing or avoid

detection of billing fraud; communications between or among BAKER, BONDS, JOHNSON, DELGADO, WASHINGTON, and COLE, and other owners or coordinators participating in the fraud; communications between the targets and their clients;

- (b) Evidence indicating how and when the Facebook account was accessed or used, to determine the chronological and geographic context of account access, use, and events relating to the crime under investigation and to the Facebook account owner;
- (c) Evidence indicating the Facebook account owner's state of mind as it relates to the crime under investigation;
- (d) The identity of the person(s) who created or used the user ID, including records that help reveal the whereabouts of such person(s).

This warrant authorizes a review of electronically stored information, communications, other records, and information disclosed pursuant to this warrant in order to locate evidence, fruits, and instrumentalities described in this warrant. The review of this electronic data may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to this warrant, IRS-CI may deliver a complete copy of the disclosed electronic data to the custody and control of attorneys for the government and their support staff for their independent review.

UNITED STATES DISTRICT COURT

for the

Eastern District of Wisconsin

A TRUE COPY

Jun 23, 2023

s/ Erin Hayes

Deputy Clerk, U.S. District Court
Eastern District of Wisconsin

In the Matter of the Search of

(Briefly describe the property to be searched
or identify the person by name and address)information associated with six (6) Facebook accounts,
described further in Attachment A, that is stored at
premises controlled by Meta Platforms, Inc.

Case No.

23-m-405 (SCD)

APPLICATION FOR A WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (identify the person or describe the property to be searched and give its location):

See Attachment A

located in the _____ District of _____, there is now concealed (identify the person or describe the property to be seized):

See Attachment B

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- ☒ evidence of a crime;
☐ contraband, fruits of crime, or other items illegally possessed;
☐ property designed for use, intended for use, or used in committing a crime;
☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section
 18 U.S.C. §§ 1956(b), 1957,
 1347, 1035 and 42 U.S.C.
 Section 1320a-7b

Offense Description
 Laundering of Monetary Instruments, Engaging in Monetary Transactions in
 Property Derived from Specified Unlawful Activity, Healthcare Fraud, False
 Statements Related to Healthcare, and Illegal Kickbacks

The application is based on these facts:

See Affidavit

- ☐ Continued on the attached sheet.
☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under
 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Jeremy Grobart
 Applicant's signature

IRS-CI Special Agent Jeremy Grobart

Printed name and title

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by
 _____ telephone _____ (specify reliable electronic means).

Date: 6-23-23

Stephen C. Dries
 Judge's signature

City and state: Milwaukee, Wisconsin

U.S. Magistrate Judge Stephen C. Dries

**AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR A SEARCH WARRANT**

I, Jeremy Grobart, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application for a search warrant for information associated with certain Facebook accounts that are stored at premises owned, maintained, controlled, or operated by Meta Platforms, Inc. (“Meta”), a company headquartered in Menlo Park, California. The information to be searched is described in the following paragraphs and in Attachment A. This affidavit is made in support of an application for a search warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A) to require Meta to disclose to the government records and other information in its possession, pertaining to the subscriber or customer associated with the account.

2. I am a Special Agent with the Criminal Investigation Division of the Internal Revenue Service (IRS-CI), United States Department of the Treasury, and have been since July of 2021. Prior to being a Special Agent with IRS-CI, I worked as a Police Officer in the City of Madison, Wisconsin from May of 2018 through July of 2021 and held a professional certification as a Certified Fraud Examiner, through the Association of Certified Fraud Examiners. I have a Bachelor’s degree in Criminal Justice from University of Cincinnati, along with an MBA with a concentration in Data Analytics from Loyola University Chicago. I have completed the Criminal Investigator Training Program and the Special Agent Investigative Techniques Program at the Federal Law Enforcement Training Center in Glynco, Georgia where I received extensive training on financial investigative techniques. My training included lessons in cybercrime investigations, virtual currency, financial investigative techniques, accounting, tax, money laundering, criminal investigation techniques, criminal law, and search warrants.

3. During this investigation, I have worked closely with IRS-CI Special Agent Zachary Stegenga, who has been employed by IRS-CI since 2008. Since 2008, Special Agent Stegenga has conducted numerous investigations involving violations of the Internal Revenue Code (Title 26, United States Code), the Money Laundering Control Act (Title 18, United States Code), the Bank Secrecy Act (Title 31, United States Code), and other related offenses. Special Agent Stegenga has been the affiant on numerous search warrants, including having participated in the execution of numerous search warrants. I have based my conclusions in part on the training and expertise of Special Agent Stegenga.

4. During this investigation, I have also consulted with Lamont Crockett, a Special Agent (SA) with the Wisconsin Department of Justice, Division of Criminal Investigation, assigned to the Wisconsin Department of Justice Medicaid Fraud Control and Elder Abuse Unit (MFCEAU). SA Crockett has worked with MFCEAU since March of 2021. He has conducted numerous investigations involving healthcare fraud and illegal kickbacks in the healthcare industry. Further, he has previously applied for warrants to search and seize evidence from social media accounts in connection with criminal healthcare investigations. I have based my conclusions in part on the training and expertise of SA Crockett.

5. I make this affidavit in support of an application for a search warrant for information associated with:

- I. Facebook Account: **Latonya Baker**, URL: **www.facebook.com/fergusonbaker**
(Target Account 1)
- II. Facebook Account: **Melissa Bonds**, URL: **www.facebook.com/melissa.bonds.92**
(Target Account 2)

- III. Facebook Account: **Grisel Delgado**, URL: **www.facebook.com/mills.finest1**
(Target Account 3)
- IV. Facebook Account: **Inez Johnson**, URL: **www.facebook.com/inez.a.johnson**
(Target Account 4)
- V. Facebook Account: **Alicia Washington**, URL:
www.facebook.com/alicia.sanders.967 (Target Account 5)
- VI. Facebook Account: **Eili J. Bliss**, URL: **www.facebook.com/eilij.cole** (Target
Account 6)

Information pertaining to these accounts is stored at premises owned, maintained, controlled, or operated by Meta Platforms (“Meta”), a social networking company headquartered at 1601 Willow Road, Menlo Park, California, 94025 (the “Target Provider”), further described herein and in Attachment A respectively (attached hereto and incorporated herein).

6. This affidavit is made in support of an application for a search warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A) to require the Target Provider to disclose to the government records and other information in its possession, including the contents of communications, pertaining to the subscriber and customer associated with all of the target accounts, further described in Section I of Attachment B (attached hereto and incorporated herein). Upon receipt of the information described in Section I of Attachment B, government-authorized persons will review that information to locate and seize the items described in Section II of Attachment B.

7. Based on my training and experience and the facts set forth in this affidavit, there is probable cause to believe that violations of 18 U.S.C. § 1956(b) (Laundering of Monetary Instruments), 18 U.S.C. § 1957 (Engaging in monetary transactions in property derived from

specified unlawful activity), 18 U.S.C. §1347 (Healthcare Fraud), 18 U.S.C. § 1035 (False Statements Related to Healthcare), and 42 U.S.C. Section 1320a-7b (Illegal Kickbacks) have been committed, are being committed, or will be committed by **LATONYA BAKER (BAKER) (DOB: 6/2/1977), MELISSA BONDS (BONDS) (DOB: 9/19/1972), INEZ JOHNSON (JOHNSON) (DOB: 9/13/1976), GRISEL DELGADO (DELGADO) (DOB: 8/14/1981), ALICIA WASHINGTON (WASHINGTON) (DOB: 7/18/1976), SHANTERA COLE (COLE) (DOB: 2/24/1995)**; and others known and unknown to the case agents. There is also probable cause to believe that the information described in Attachment B will constitute evidence of these criminal violations and will lead to the identification of individuals who are engaged in the commission of these offenses.

8. The facts in this affidavit come from my personal observations, my training and experience, information obtained from other agents and witnesses, public records, and my own investigative efforts. I believe these sources of information to be credible and reliable based on the corroboration of the information and my experience with these matters. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all my knowledge about this matter.

9. This Court has jurisdiction to issue the requested warrant because it is “a court of competent jurisdiction” as defined by 18 U.S.C. § 2711. 18 U.S.C. §§ 2703(a), (b)(1)(A) & (c)(1)(A). Specifically, the Court is “a district court of the United States . . . that – has jurisdiction over the offense being investigated.” 18 U.S.C. § 2711(3)(A)(i).

PROBABLE CAUSE

Background about PNCC and CCC Programs

10. Prenatal Care Coordination (PNCC) and Child Care Coordination (CCC) benefits help provide access to medical, social, and educational resources for women who are considered at high risk for adverse pregnancy outcomes, and for their children after the pregnancy. The components of this benefit are outreach, assessment, care plan development, ongoing care coordination and monitoring, and health education and nutrition counseling.

11. PNCC and CCC services are reimbursed by Wisconsin Medicaid when provided in accordance with Wisconsin Medicaid's rules and regulations. Covered services related to the benefit are listed in Wis. Admin. Code § DHS 107.34 and the Forward Health Online Handbook.

12. When enrolling in Wisconsin Medicaid, owners of agencies providing PNCC and CCC services sign a provider agreement. The provider agreement states that every time a provider submits a claim, the provider is certifying that he or she has not offered, paid, or received any type of illegal remuneration in violation of 42 U.S.C. § 1320a-7b, Wis. Stat. § 946.91(3).

13. The PNCC and CCC programs require providers to submit accurate and truthful claims for payments. The programs also require a provider to only seek reimbursement for the actual amount of time spent assisting a member. And they prohibit providers from seeking reimbursement for non-covered services. The Wisconsin Department of Health Services (DHS) provides that if a client needs something like diapers or wipes, a care coordinator should connect the client with an organization that can provide those items, rather than providing them directly. Both programs prohibit seeking reimbursement for noncovered services by charging for a covered service that was not actually provided.

14. Per Wis. Admin. Code § DHS 107.34, PNCC and CCC agencies are required to work with a Qualified Professional, who is either a CNP, licensed nurse, midwife, dietician, RN with two or more years of appropriate experience, a PA, or a health educator with a master's degree or two or more years of relevant experience. Prior to services being performed for a Medicaid recipient by a PNCC, and the subsequent reimbursement by Wisconsin Medicaid, an initial assessment and care plan are required. The Qualified Professional reviews and signs the assessment.

15. DHS maintains an online portal that allows for the submission of allegations of fraud involving Wisconsin Medicaid-funded providers. This online portal assists DHS in its mission to identify and investigate Wisconsin Medicaid fraud.

Background about the Investigation

16. Between August 2019 and October 2021, GENERATION OF EXCELLENCE PRENATAL CARE (GOEPC) received \$2,180,286.80 from Wisconsin Medicaid, which was among the highest in the state. JMJ CONSULTING LLC (JMJ) went from receiving approximately \$1,926.35 in 2020 to receiving \$607,211.79 by October 2021.

Generation of Excellence Prenatal Care (GOEPC)

17. GOEPC was enrolled as a Prenatal Care provider with Wisconsin Medicaid on April 23, 2019, and dissolved on September 20, 2021. Records from WI DHS, Wisconsin Department of Financial Institutions (DFI), Milwaukee County Circuit Court, and publicly available Facebook posts, show that WASHINGTON, COLE, and BAKER were the shared owners of GOEPC. BAKER was also listed as the managing employee for GOEPC on the Wisconsin Medicaid Provider Enrollment Report.

18. On January 27, 2022, the Wisconsin Department of Health Services Office of the Inspector General (WI DHS-OIG), received a complaint about GOEPC. The complaint alleged that GOEPC and its owner, BAKER, were illegally offering sign-on bonuses to prospective clients. BAKER had been posting about these bonuses on her Facebook page.

19. A review of Facebook posts on **Target Account 1, Target Account 5, and Target Account 6** revealed advertisements for events at which women would receive free baby-related supplies (examples are provided below). When women came to, or registered for, these events to receive their items, they were required to provide their identifying information and/or enroll in GOEPC's PNCC and CCC programs. GOEPC would then utilize the identifying information to submit bills to Medicaid. By providing free items to induce women to join the GOEPC's PNCC and CCC programs, GOEPC violated the Anti-kickback statutes.

Generation of Excellence Trendsetters (GOET) and JMJ Prenatal Care (JMJ)

20. GOEPC dissolved in September 2021. Prior to its dissolution, BAKER applied with WI DHS to start another Prenatal Care agency called GENERATION OF EXCELLENCE TRENDSETTERS (GOET). BAKER submitted her first application to WI DHS for GOET on March 22, 2021. BAKER's application was rejected twice because she lacked a proper "Qualified Professional."

21. BAKER's GOET application was ultimately approved on November 22, 2022. Once GOET's application was approved, BAKER was eligible to seek reimbursement for services provided to clients as of the date of GOET's application: May 4, 2022.

22. Between September 2021 and November 2022 (after GOEPC had dissolved and before GOET's application to become a Prenatal Care provider had been approved), BAKER partnered with BONDS, whose company JMJ, had been an approved PNCC and CCC provider

since July 9, 2019. In the summer of 2021, BAKER and BONDS formed a shared business venture called “JMJ Prenatal Care and GOE Trendsetters Better Together.”

23. BAKER used that joint venture to advertise Prenatal Care being offered by GOET, even though GOET was not approved by the state to provide such services. BAKER used these advertisements to gain access to new clients and their Wisconsin Medicaid numbers. BAKER used that information to submit fraudulent PNCC and CCC claims to Wisconsin Medicaid through JMJ and not GOET.

24. Although GOET was not authorized to provide PNCC and CCC services, \$1,778,026.25 of the \$4,283,763.89 paid by Wisconsin Medicaid to JMJ between June 18, 2021 and November 25, 2022 was deposited directly into a GOET business bank account controlled by BAKER and JOHNSON. Prior to that time period, between December 23, 2019 and June 17, 2021, JMJ received just \$9,532.64 from Wisconsin Medicaid for PNCC and CCC services.

25. Agents conducted physical surveillance and were able to determine that the GOET and JMJ partnership operated out of three locations: 6633 W. Mill Rd Milwaukee, WI 53218 (Northside Office), 2222 Mayfair Rd Wauwatosa, WI 53226 (Westside Office), and 7143 W. Greenfield Ave West Allis, WI 53204 (Southside Office). DHS records and Facebook posts showed DELGADO being the Director of Operations for the GOET Southside Office and JOHNSON being the Director Operations for the GOET Westside Office. Both DELGADO and JOHNSON worked with BAKER at GOEPC and are believed have assisted BAKER in fraudulently billing Wisconsin Medicaid while acting as GOET executives.

Fraudulent Billing Data

26. PNCC and CCC billing records for GOEPC and JMJ, maintained by WI DHS, contain multiple indicators of fraud. Between January 14, 2020, and October 1, 2021, \$199,396.94

in GOEPC claims that were paid by Wisconsin Medicaid contained duplicate billing, meaning that two PNCC/CCC providers submitted claims for services provided to the same client.

27. Similarly, for MJJ, between February 20, 2021, and February 28, 2022, \$189,305.87 in MJJ claims that were paid by Wisconsin Medicaid contained duplicate billing.

28. The program rules make clear that it is the provider's responsibility to ensure that the client is not receiving PNCC or CCC services from other providers. Providers can confirm that no other entity is providing services by completing an enrollment check.

29. WI DHS records show that GOEPC completed no enrollment checks for 126 (or 19.4%) of its clients. MJJ completed no enrollment checks for 801 (or 41.8%) of its clients.

30. Wisconsin Medicaid requires providers to list the name of the Care Coordinator administering PNCC or CCC services to clients. Between October 2021 and March 2022, MJJ received \$267,773.08 in claim payments for claims that did not list any Care Coordinator.

31. Other claims that did list the Care Coordinator showed that between October 2021 and March 2022, MJJ received \$266,107.68 from Wisconsin Medicaid as a result of billing for "impossible days." An "impossible day" is a day in which a provider's claims, if accurate, would have meant that the provider worked more than 24 hours a day. For example, claims submitted by MJJ included 30 days on which JOHNSON had supposedly worked "impossible days." Some of those "impossible days" included claims that meant Johnson worked:

- i. 128 hours on October 23, 2021.
- ii. 120 hours on November 22, 2021.
- iii. 120 hours on December 20, 2021.
- iv. 128 hours on January 17, 2022
- v. 126 hours on February 22, 2022.

32. GOEPC and JMJ also frequently submitted bills asserting that they had provided the maximum amount of service permissible under the program (i.e., 10 hours per month). Indeed, a majority of claims submitted by GOEPC and JMJ included claims billed at, or above, the maximum. Because Wisconsin Medicaid requires providers to bill only for the amount of time they actually spend providing covered services, billing a majority of claims at the maximum allowable is an indicator of fraudulent billing.

Analysis of Bank Records

33. Agents analyzed bank records from an Associated Bank business account belonging to GOET. BAKER and JOHNSON were listed as signors on the account. Between July 15, 2021, and March 24, 2022, \$1,778,026.25 in Wisconsin Medicaid funds were deposited into the account “for the benefit of JMJ Consulting.” These were the only deposits into that account. WI DHS-OIG Investigators advised agents that GOET should not have been receiving any Wisconsin Medicaid deposits during that time period. Bank records show that these funds were never transferred to JMJ. Instead, numerous checks, from the GOET account, were written to JOHNSON, DELGADO, BAKER, and BONDS for various things such as payroll and reimbursement of other expenses. Between August 7, 2021 and July 1, 2022 \$1,041,557.42 of the money deposited by Wisconsin Medicaid, into the GOET bank account, went to Paycor; \$395,075.33 of that was paid to BAKER, JOHNSON, DELGADO, and BONDS.

34. Between July 8, 2022, and November 25, 2022, \$2,265,068.16 in Wisconsin Medicaid payments were deposited into a JMJ bank account. Between May 5, 2022 and August 29, 2022, \$1,163,777.60 of the money deposited into JMJ’s account from Wisconsin Medicaid was immediately transferred to the GOET bank account at US Bank. Between September 1, 2022, and November 28, 2022, \$952,272.61 in Wisconsin Medicaid deposits was withdrawn from the

JMJ bank account and deposited into the GOET bank account. \$326,049.57 that was deposited into MJJ's US Bank account from Wisconsin Medicaid and then moved to GOET's US Bank account, ultimately ended up in personal bank accounts belonging to BAKER and JOHNSON. GOET was not authorized to provide, or bill for, services to Wisconsin Medicaid during these time periods. GOET was not, therefore, permitted to receive these Wisconsin Medicaid funds.

35. An analysis of these bank records revealed that the targets used the fraudulently obtained Medicaid funds to pay for expensive vacations such as trips to Dubai, Bahamas, Puerto Rico, Las Vegas. They also used the money to buy luxury items, and to fund other, unrelated businesses owned by BAKER.

DHS Fraud Complaints

36. On February 10, 2023, DHS-OIG received a fraud complaint regarding MJJ. The complainant, K.V., works for a non-profit in the Milwaukee, WI area that provides PNCC and CCC services to expectant mothers and children. K.V. was made aware of a duplicate billing issue involving a client receiving services from K.V.'s agency. K.V. was told by WI DHS that MJJ was billing Wisconsin Medicaid for CCC services, using K.V.'s client's Medicaid number. K.V.'s client had not received any services from MJJ.

37. Agents interviewed K.V. and her client, O.B., on March 29, 2023. O.B. told agents that when she was pregnant with her youngest son, B.B., a friend connected O.B. with a Prenatal Care Coordinator named Tabitha. O.B. never knew Tabitha's last name but provided agents with Tabitha's phone number, which is 414-406-7245. Agents have identified Tabitha as Tabitha L. Bates. Tabitha's public Facebook page features MJJ, GOET, and BAKER.

38. O.B. told agents that Tabitha first texted her on September 20, 2021. Tabitha told O.B. that she was her Care Coordinator and would be helping O.B. throughout her pregnancy with

B.B. Per Tabitha's request, O.B. sent Tabitha a picture of O.B.'s Wisconsin Medicaid number. O.B. was never asked any questions about her health or pregnancy, nor was O.B. provided any documents to sign.

39. O.B. heard from Tabitha only intermittently after that. For example, they exchanged texts on January 7, 2022 when Tabitha indicated she had a welcome package and paperwork for O.B. Tabitha never followed up or provided the welcome package. In March 2022, O.B. contacted Tabitha to tell her she was hospitalized and would be induced on April 4, 2022. On April 7, 2022, Tabitha contacted O.B. to ask her if she was ready to deliver B.B., and on May 18, 2022 Tabitha asked for B.B.'s Medicaid number, which O.B. provided. On that same day, Tabitha had scheduled a time to deliver diapers to O.B. but again never came or followed-up with O.B. Tabitha also texted to offer diapers on June 25, 2022, August 19, 2022 and February 23, 2023, but never delivered diapers.

40. O.B. told agents that she never saw Tabitha in person and was not provided any PNCC or CCC services by Tabitha or any other Care Coordinator from JMJ. Despite that, JMJ submitted twenty claims to Wisconsin Medicaid for PNCC services supposedly provided to O.B. between September 6, 2021 and February 16, 2022. JMJ also submitted twenty five claims to Wisconsin Medicaid for CCC services supposedly provided to B.B. between April 4, 2022 and August 16, 2022. O.B. was unaware that JMJ was billing the state for services supposedly provided to her by Tabitha.

Facebook Accounts

41. Agents utilized an undercover Facebook account to determine that BAKER, BONDS, JOHNSON, DELGADO, WASHINGTON, and COLE were using their own Facebook accounts to promote GOEPC and JMJ. A review of those accounts also revealed that BAKER,

BONDS, JOHNSON, DELGADO, WASHINGTON, and COLE used Facebook to offer illegal incentives, remuneration, and kickbacks to induce clients to register in the program so that they could bill Medicaid for services purportedly provided to those clients. The following examples were identified by agents:

Target Account 1

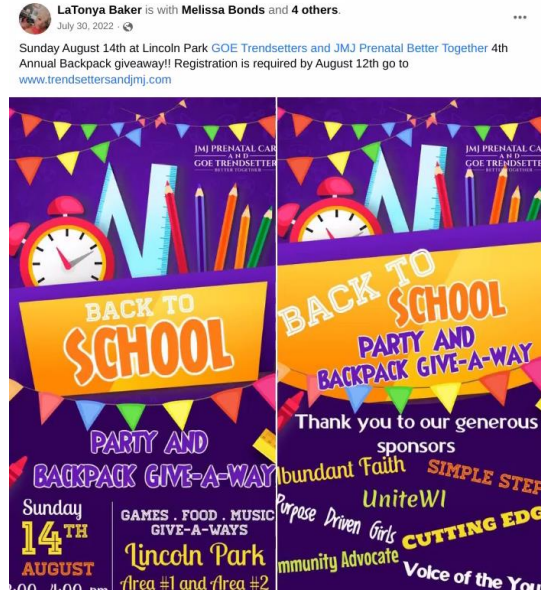
42. On April 23, 2020, **Target Account 1**, belonging to BAKER, posted a flyer advertising a \$500 giveaway from GOEPC. On the post, it stated that for someone to win the \$500, they must “share the live video, follow and like the GOEPC page, be a single parent, and be unemployed.”

TARGET ACCOUNT 1 Facebook Post from April 23, 2020



43. On July 30, 2022, **Target Account 1** posted a flyer for a “Back to School Backpack Give-A-Way” hosted by “JMJ Prenatal Care and GOE Trendsetters”. To receive a backpack, registration with JMJ was required. **Target Account 2** which Meta Inc. records confirm belongs to BONDS, was also tagged in this post. A screenshot of the post is below:

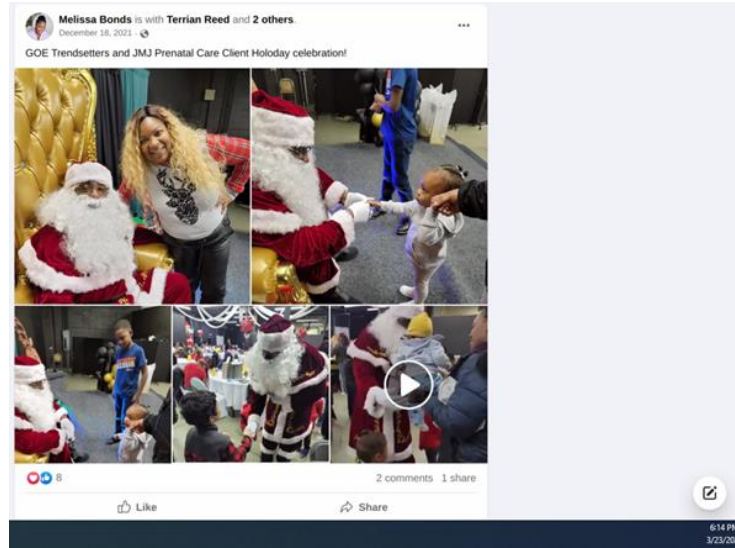
TARGET ACCOUNT 1 Facebook Post from July, 30, 2022



Target Account 2

44. **Target Account 2** included a post from December 18, 2021, which had photos from the “GOE Trendsetters and JMJ Prenatal Care Client Holiday celebration.” The post contained photos of children, tables full of toys, and an individual dressed as Santa Claus posing for pictures. Baker had commented on the post saying “Today was amazing!!” Agents believe that the post advertised a Christmas giveaway that was used to incentivize others to enroll with JMJ. A screenshot of the post is below:

TARGET ACCOUNT 2 Facebook Post from December 18, 2021



Target Account 3

45. On April 26, 2021, **Target Account 3**, which Meta Inc. has confirmed belongs to DELGADO, shared a Facebook post of a flyer for an event that was initially posted by **Target Account 1**. The flyer promoted the grand opening of Generation of Excellence Trendsetters Southside and said that “GOET is expanding their prenatal care coordinating services to Milwaukee’s Southside!” and “each mom will receive a special gift and a delicious Mother’s Day Dinner.” Attendees had to RSVP with DELGADO, whose phone number was listed at the bottom of the flyer. This post advertised GOET as a Prenatal Care provider despite them not being licensed as such by WI DHS. A screenshot of the Facebook post on **Target Account 3** is below:

TARGET ACCOUNT 3 Facebook Post from on April 26, 2021



46. On August 7, 2022, multiple pictures were posted on **Target Account 3** saying “JMJ Prenatal & GOE Trendsetters South is at Puerto Rican Family Festival. We have prizes [agents believe this was meant to be “prizes”]. Come visit us to get our raffle tickets. First raffle times as follow: 2pm, 4pm, and 6pm.” A screenshot of the Facebook post on **Target Account 3** is below:

TARGET ACCOUNT 3 Facebook post from August 7, 2022



Target Account 4

47. Agents then viewed **Target Account 4**, which Meta Inc. has confirmed belongs to JOHNSON. On the homepage of **Target Account 4**, agents saw that JOHNSON's employment was listed as with "GOE Trendsetters Westside." On January 26, 2022, **Target Account 4** posted a flyer advertising the "Generation of Excellence Trendsetters South 1st Annual Share the Warmth winter hat, scarf, and glove drive." During this time period, GOET had been advertising itself as a PNCC and CCC provider through its partnership with JMJ. The location of this event, 7143 W. Greenfield Avenue West Allis, WI, is the same location where **Target Account 3** had previously advertised the launch of prenatal services.

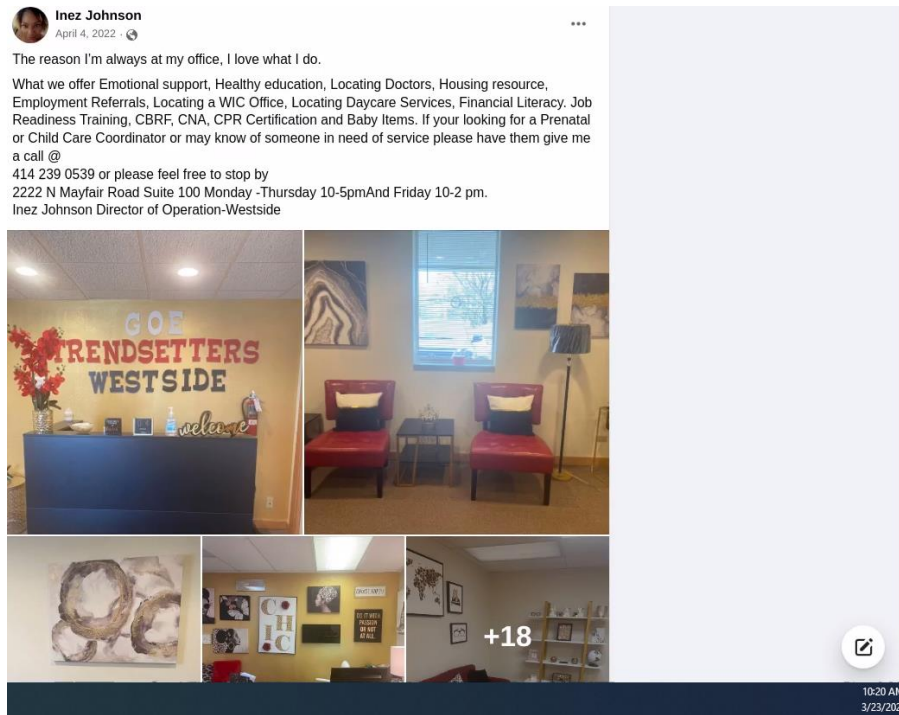
48. Furthermore, on April 4, 2022, **Target Account 4** was used to post about JOHNSON's new position as the Director of Operations for GOE TRENDSETTERS WESTSIDE. In the post, JOHNSON stated "If you're looking for a Prenatal or Child Care Coordinator or may know of someone in need of service, please have them give me a call at 414-239-0539 or please

feel free to stop by 2222 N Mayfair Rd Suite 100.” **Target Account 4** was again being used to promote GOET, and this time stated that GOET was a Prenatal Care agency. However, WI DHS records show that at this time, GOET was not an approved provider of PNCC and CCC services even though money from Wisconsin Medicaid was being deposited into a GOET business bank account. Thus, **Target Account 4** was not only being used to incentivize potential PNCC and CCC clients through a clothing giveaway, but to falsely advertise GOET as a PNCC and CCC provider. Screenshots of both posts are below:

TARGET ACCOUNT 4 Facebook Post January 26, 2022



TARGET ACCOUNT 4 Facebook Post April 4, 2022



Target Account 5

49. Agents then viewed **Target Account 5**, which Meta Inc. has confirmed belongs to WASHINGTON. On January 22, 2020, **Target Account 5** posted a flyer advertising a “Community Baby Shower.” The flyer stated that clients had to register to receive “a customized bag of FREE baby items.” The post on **Target Account 5** stated that “GOE has partnered with Aurora Health Care and COA to bring to you a Community Baby Shower!!” This post shows **Target Account 5** being used to illegally incentivize potential clients to enroll with GOEPC by offering free gifts. A screenshot of the post is below:

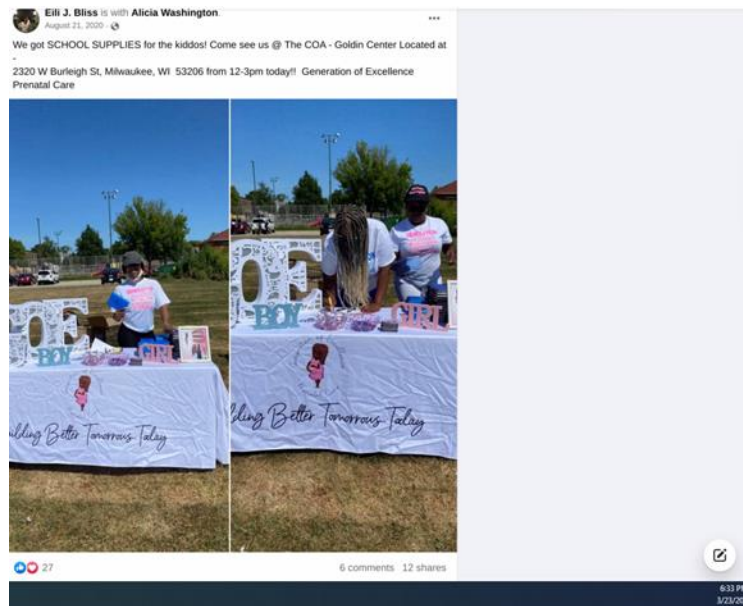
Target Account 5 Facebook Post from January 22, 2020



Target Account 6

50. The final Facebook account that agents viewed was **Target Account 6**, which Meta Inc. has confirmed belongs to COLE. On August 21, 2020, multiple pictures of COLE and WASHINGTON behind a GOEPC table with school supplies were posted on **Target Account 6**. The post stated that “We got SCHOOL SUPPLIES for the kiddos! Come see us @ The COA-Goldin Center Located at 1320 W. Burleigh St, Milwaukee, WI 53206 from 12-3pm today!! Generation of Excellence Prenatal Care.” Similar to all of the other posts, this post shows **Target Account 6** being used to illegally incentivize potential clients to enroll with GOEPC by offering free giveaways. A screenshot of the post is below:

Target Account 6 Facebook Post from August 21, 2020



51. These posts show the target Facebook accounts were being used to advertise GOEPC and JMJ and also to offer illegal kickbacks, on behalf of GOEPC and JMJ. Furthermore, the posts refer to GOET as a PNCC and CCC provider despite it not being an approved provider. These posts show, therefore, that evidence of fraud will likely be found on the Facebook pages of the Target Accounts, which are connected to BAKER, JOHNSON, BONDS, DELGADO, WASHINGTON, and COLE. Such evidence will likely include communications between BAKER, JOHNSON, BOND, DELGADO, WASHINGTON, and COLE and other potential targets of the investigation, along with statements about BAKER, JOHNSON, BONDS, DELGADO, WASHINGTON, and COLE's knowledge of, and profit from, the scheme. It will also likely include the target's communications with potential clients.

BACKGROUND CONCERNING FACEBOOK¹

52. Meta owns and operates Facebook, a free-access social networking website that can be accessed at <http://www.facebook.com>. Facebook users can use their accounts to share communications, news, photographs, videos, and other information with other Facebook users, and sometimes with the general public.

53. Meta asks Facebook users to provide basic contact and personal identifying information either during the registration process or thereafter. This information may include the user's full name, birth date, gender, e-mail addresses, physical address (including city, state, and zip code), telephone numbers, screen names, websites, and other personal identifiers. Each Facebook user is assigned a user identification number and can choose a username.

54. Facebook users may join one or more groups or networks to connect and interact with other users who are members of the same group or network. Facebook assigns a group identification number to each group. A Facebook user can also connect directly with individual Facebook users by sending each user a "Friend Request." If the recipient of a "Friend Request" accepts the request, then the two users will become "Friends" for purposes of Facebook and can exchange communications or view information about each other. Each Facebook user's account includes a list of that user's "Friends" and a "News Feed," which highlights information about the user's "Friends," such as profile changes, upcoming events, and birthdays.

¹ The information in this section is based on information published by Meta on its Facebook website, including, but not limited to, the following webpages: "Privacy Policy," available at <https://www.facebook.com/privacy/policy>; "Terms of Service," available at <https://www.facebook.com/legal/terms>; "Help Center," available at <https://www.facebook.com/help>; and "Information for Law Enforcement Authorities," available at <https://www.facebook.com/safety/groups/law/guidelines/>.

55. Facebook users can select different levels of privacy for the communications and information associated with their Facebook accounts. By adjusting these privacy settings, a Facebook user can make information available only to himself or herself, to particular Facebook users, or to anyone with access to the Internet, including people who are not Facebook users. A Facebook user can also create “lists” of Facebook friends to facilitate the application of these privacy settings. Facebook accounts also include other account settings that users can adjust to control, for example, the types of notifications they receive from Facebook.

56. Facebook users can create profiles that include photographs, lists of personal interests, and other information. Facebook users can also post “status” updates about their whereabouts and actions, as well as links to videos, photographs, articles, and other items available elsewhere on the Internet. Facebook users can also post information about upcoming “events,” such as social occasions, by listing the event’s time, location, host, and guest list. In addition, Facebook users can “check in” to particular locations or add their geographic locations to their Facebook posts, thereby revealing their geographic locations at particular dates and times. A particular user’s profile page also includes a “Wall,” which is a space where the user and his or her “Friends” can post messages, attachments, and links that will typically be visible to anyone who can view the user’s profile.

57. Facebook users can upload photos and videos to be posted on their Wall, included in chats, or for other purposes. Users can “tag” other users in a photo or video, and can be tagged by others. When a user is tagged in a photo or video, he or she generally receives a notification of the tag and a link to see the photo or video.

58. Facebook users can use Facebook Messenger to communicate with other users via text, voice, video. Meta retains instant messages and certain other shared Messenger content

unless deleted by the user, and also retains transactional records related to voice and video chats. Facebook users can also post comments on the Facebook profiles of other users or on their own profiles; such comments are typically associated with a specific posting or item on the profile.

59. If a Facebook user does not want to interact with another user on Facebook, the first user can “block” the second user from seeing his or her account.

60. Facebook has a “like” feature that allows users to give positive feedback or connect to particular pages. Facebook users can “like” Facebook posts or updates, as well as webpages or content on third-party (*i.e.*, non-Facebook) websites. Facebook users can also become “fans” of particular Facebook pages.

61. Facebook has a search function that enables its users to search Facebook for keywords, usernames, or pages, among other things.

62. Each Facebook account has an activity log, which is a list of the user’s posts and other Facebook activities from the inception of the account to the present. The activity log includes stories and photos that the user has been tagged in, as well as connections made through the account, such as “liking” a Facebook page or adding someone as a friend. The activity log is visible to the user but cannot be viewed by people who visit the user’s Facebook page.

63. Facebook also has a Marketplace feature, which allows users to post free classified ads. Users can post items for sale, housing, jobs, and other items on the Marketplace.

64. In addition to the applications described above, Meta provides users with access to thousands of other applications (“apps”) on the Facebook platform. When a Facebook user accesses or uses one of these applications, an update about that the user’s access or use of that application may appear on the user’s profile page.

65. Meta also retains records of which IP addresses were used by an account to log into or out of Facebook, as well as IP address used to take certain actions on the platform. For example, when a user uploads a photo, the user's IP address is retained by Meta along with a timestamp.

66. Meta retains location information associated with Facebook users under some circumstances, such as if a user enables "Location History," "checks-in" to an event, or tags a post with a location.

67. Social networking providers like Meta typically retain additional information about their users' accounts, such as information about the length of service (including start date), the types of service utilized, and the means and source of any payments associated with the service (including any credit card or bank account number). In some cases, Facebook users may communicate directly with Meta about issues relating to their accounts, such as technical problems, billing inquiries, or complaints from other users. Social networking providers like Meta typically retain records about such communications, including records of contacts between the user and the provider's support services, as well as records of any actions taken by the provider or user as a result of the communications.

68. As explained herein, information stored in connection with a Facebook account may provide crucial evidence of the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, a Facebook user's IP log, stored electronic communications, and other data retained by Meta, can indicate who has used or controlled the Facebook account. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. For example, profile contact information, private messaging logs, status updates, and tagged

photos (and the data associated with the foregoing, such as date and time) may be evidence of who used or controlled the Facebook account at a relevant time. Further, Facebook account activity can show how and when the account was accessed or used. For example, as described herein, Meta logs the Internet Protocol (IP) addresses from which users access their accounts along with the time and date. By determining the physical location associated with the logged IP addresses, investigators can understand the chronological and geographic context of the account access and use relating to the crime under investigation. Such information allows investigators to understand the geographic and chronological context of Facebook access, use, and events relating to the crime under investigation. Additionally, location information retained by Meta may tend to either inculcate or exculpate the Facebook account owner. Last, Facebook account activity may provide relevant insight into the Facebook account owner's state of mind as it relates to the offense under investigation. For example, information on the Facebook account may indicate the owner's motive and intent to commit a crime (e.g., information indicating a plan to commit a crime), or consciousness of guilt (e.g., deleting account information in an effort to conceal evidence from law enforcement).

69. Therefore, the servers of Meta are likely to contain all the material described above, including stored electronic communications and information concerning subscribers and their use of Facebook, such as account access information, transaction information, and other account information.

CONCLUSION

70. Based on the foregoing, I request that the Court issue the proposed search warrant.

71. I anticipate executing this warrant under the Electronic Communications Privacy Act, in particular 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A), by using the warrant to

require Meta to disclose to the government copies of the records and other information (including the content of communications) particularly described in Section I of Attachment B. Upon receipt of the information described in Section I of Attachment B, government-authorized persons will review that information to locate the items described in Section II of Attachment B.

72. Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for the service or execution of this warrant. The government will execute this warrant by serving it on Meta. Because the warrant will be served on Meta, who will then compile the requested records at a time convenient to it, reasonable cause exists to permit the execution of the requested warrant at any time in the day or night.

ATTACHMENT A

Property to Be Searched

This warrant applies to information associated with Facebook accounts:

- I. **Facebook Account: Latonya Baker, URL: www.facebook.com/fergusonbaker
(Target Account 1)**
- II. **Facebook Account: Melissa Bonds, URL:
www.facebook.com/melissa.bonds.92 (Target Account 2)**
- III. **Facebook Account: Grisel Delgado, URL: www.facebook.com/mills.finest1
(Target Account 3)**
- IV. **Facebook Account: Inez Johnson, URL: www.facebook.com/inez.a.johnson
(Target Account 4)**
- V. **Facebook Account: Alicia Washington, URL:
www.facebook.com/alicia.sanders.967 (Target Account 5)**
- VI. **Facebook Account: Eili J. Bliss, URL: www.facebook.com/eilij.cole (Target
Account 6)**

which are stored at premises owned, maintained, controlled, or operated by Meta Platforms, Inc., a company headquartered in Menlo Park, California.

ATTACHMENT B

Particular Things to be Seized

I. Information to be disclosed by Meta Platforms, Inc. (“Meta”)

To the extent that the information described in Attachment A is within the possession, custody, or control of Meta, regardless of whether such information is located within or outside of the United States, including any messages, records, files, logs, or information that have been deleted but are still available to Meta, or have been preserved pursuant to a request made under 18 U.S.C. § 2703(f), Meta is required to disclose the following information to the government for each user ID listed in Attachment A **for the time period of April 23, 2020, through the date of this warrant for Target Account 1, December 18, 2021, through the date of this warrant for Target Account 2, April 6, 2021, through the date of this warrant for Target Account 3, January 26, 2022, through the date of this warrant for Target Account 4, January 22, 2020 through the date of this warrant for Target Account 5, and August 21, 2020, through the date of this warrant for Target Account 6.**

- (a) All contact and personal identifying information, including full name, user identification number, birth date, gender, contact e-mail addresses, physical address (including city, state, and zip code), telephone numbers, screen names, websites, and other personal identifiers.
- (b) All activity logs for the account and all other documents showing the user’s posts and other Facebook activities from April 23, 2020, through the date of this warrant for Target Account 1, December 18, 2021, through the date of this warrant for Target Account 2, April 6, 2021, through the date of this warrant for Target Account 3, January 26, 2022, through the date of this warrant for Target Account 4, January

22, 2020 through the date of this warrant for Target Account 5, and August 21, 2020, through the date of this warrant for Target Account 6.

- (c) All photos and videos uploaded by that user ID and all photos and videos uploaded by any user that have that user tagged in them from April 23, 2020, to present for Target Account 1, December 18, 2021, to present for Target Account 2, April 6, 2021, to present for Target Account 3, January 26, 2022, to present for Target Account 4, January 22, 2020 to present for Target Account 5, and August 21, 2020, to present for Target Account 6, including Exchangeable Image File (“EXIF”) data and any other metadata associated with those photos and videos;
- (d) All profile information; News Feed information; status updates; videos, photographs, articles, and other items; Notes; Wall postings; friend lists, including the friends’ Facebook user identification numbers; groups and networks of which the user is a member, including the groups’ Facebook group identification numbers; future and past event postings; rejected “Friend” requests; comments; gifts; pokes; tags; and information about the user’s access and use of Facebook applications;
- (e) All records or other information regarding the devices and internet browsers associated with, or used in connection with, that user ID, including the hardware model, operating system version, unique device identifiers, mobile network information, advertising ID, and user agent string;
- (f) All other records and contents of communications and messages made or received by the user from April 23, 2020, to present for Target Account 1, December 18, 2021, to present for Target Account 2, April 6, 2021, to present for Target Account 3, January 26, 2022, to present for Target Account 4, January 22, 2020 to present

for Target Account 5, and August 21, 2020, to present for Target Account 6, including all Messenger activity, private messages, chat history, video and voice calling history, and pending “Friend” requests;

- (g) All “check ins” and other location information;
- (h) All IP logs, including all records of the IP addresses that logged into the account;
- (i) All records of the account’s usage of the “Like” feature, including all Facebook posts and all non-Facebook webpages and content that the user has “liked”;
- (j) All information about the Facebook pages that the account is or was a “fan” of;
- (k) All past and present lists of friends created by the account;
- (l) All records of Facebook searches performed by the accounts from April 23, 2020, to present for Target Account 1, December 18, 2021, to present for Target Account 2, April 6, 2021, to present for Target Account 3, January 26, 2022, to present for Target Account 4, January 22, 2020, to present for Target Account 5, and August 21, 2020, to present for Target Account 6;
- (m) All information about the user’s access and use of Facebook Marketplace;
- (n) The types of service utilized by the user;
- (o) The length of service (including start date) and the means and source of any payments associated with the service (including any credit card or bank account number);
- (p) All privacy settings and other account settings, including privacy settings for individual Facebook posts and activities, and all records showing which Facebook users have been blocked by the account;

- (q) Records of any Facebook accounts that are linked to the account by machine cookies (meaning all Facebook user IDs that logged into Facebook by the same machine as the account); and
- (r) All records pertaining to communications between Meta and any person regarding the user or the user's Facebook account, including contacts with support services and records of actions taken.

Meta is hereby ordered to disclose the above information to the government within 14 days of issuance of this warrant.

II. Information to be seized by the government

All information described above in Section I that constitutes fruits, evidence and instrumentalities of violations of 18 U.S.C. § 1956(b) (Laundering of Monetary Instruments), 18 U.S.C. § 1957 (Engaging in monetary transactions in property derived from specified unlawful activity), 18 U.S.C. § 1347 (Healthcare Fraud), 18 U.S.C. § 1035 (False Statements Related to Healthcare), 42 U.S.C. Section 1320a-7b (Illegal Kickbacks) involving LATONYA BAKER, MELISSA BONDS, INEZ JOHNSON, GRISEL DELGADO, ALICIA WASHINGTON, and SHANTERA COLE since, April 23, 2020, for Target Account 1, December 18, 2021, for Target Account 2, April 6, 2021, for Target Account 3, January 26, 2022, for Target Account 4, January 22, 2020 for Target Account 5, and August 21, 2020, for Target Account 6, including, for each user ID identified on Attachment A, information pertaining to the following matters:

- (a) Evidence demonstrating a scheme to defraud Wisconsin Medicaid; evidence demonstrating the provision of kickbacks in exchange for medical services and/or billing; evidence of communications regarding how to conduct billing or avoid

detection of billing fraud; communications between or among BAKER, BONDS, JOHNSON, DELGADO, WASHINGTON, and COLE, and other owners or coordinators participating in the fraud; communications between the targets and their clients;

- (b) Evidence indicating how and when the Facebook account was accessed or used, to determine the chronological and geographic context of account access, use, and events relating to the crime under investigation and to the Facebook account owner;
- (c) Evidence indicating the Facebook account owner's state of mind as it relates to the crime under investigation;
- (d) The identity of the person(s) who created or used the user ID, including records that help reveal the whereabouts of such person(s).

This warrant authorizes a review of electronically stored information, communications, other records, and information disclosed pursuant to this warrant in order to locate evidence, fruits, and instrumentalities described in this warrant. The review of this electronic data may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to this warrant, IRS-CI may deliver a complete copy of the disclosed electronic data to the custody and control of attorneys for the government and their support staff for their independent review.